

**TWENTIETH ANNUAL
NORTHEAST SURETY AND FIDELITY
CLAIMS CONFERENCE**

SEPTEMBER 24th and 25th, 2009

**COMPUTER FRAUD COVERAGE:
AN EXAMINATION OF DEVELOPING ISSUES**

PRESENTED BY:

**SUSAN EVANS JONES, ESQUIRE
WOLF, HOROWITZ & ETLINGER, LLC**
99 Pratt Street, Suite 401
Hartford, Connecticut 06103
(860) 724-6667
Fax: (860) 293-1979

COMPUTER FRAUD COVERAGE: AN EXAMINATION OF DEVELOPING ISSUES

I. INTRODUCTION

Modern commercial crime policies generally contain various insuring agreements. One such common insuring agreement is the Computer Fraud Coverage Agreement.

A typical Computer Fraud Insuring Agreement may provide as follows:

We will pay for loss of or damage to “money”, “securities” and “other property” resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the “premises” or “banking premises”:

- a. To a person (other than a “messenger”) outside those “premises”; or
- b. To a place outside those “premises”.¹

Other policies may contain variations of this language, stating, for instance: “We will pay you for your direct loss of, or your direct loss from damage to, Money, Securities and Other Property directly caused by Computer Fraud.” “Computer Fraud” may then be defined as:

The use of any computer to fraudulently cause a transfer of Money, Securities or Other Property from inside the Premises or Banking Premises:

1. to a person . . . outside the Premises or Banking Premises; or
2. to a place outside the Premises or Banking Premises.

Or a crime policy may provide that the insurer will pay for “direct loss sustained by Insured resulting from Computer Fraud committed by a Third Party”, with “Computer Fraud” defined as “the unlawful taking of Money, Securities or Property resulting from a Computer Violation” and “Computer Violation” defined as:

. . . an unauthorized:

- (1) entry into or deletion of data from a Computer System;
- (2) change to data elements or program logic of a Computer System, which is kept in machine readable format; or
- (3) introduction of instructions, programmatic or otherwise, which propagate themselves through a Computer System;

directed solely against any Insured. . . .

These computer fraud coverage provisions are typically intended to provide coverage for “computer hacking” incidents, or losses caused when a person uses a computer to transfer money or property from the insured to another person or place. However, given the predominance of computers in everyday life, claimants may attempt to invoke the computer

¹ See ISO Form CR 00 21 07 02; ISO Form CR 00 23 05 06.

fraud insuring agreement for losses other than what is typically thought of as a computer hacking incident, based on the connection of a computer to the alleged loss.

This paper will address the computer fraud insuring agreement, various exclusions to the computer fraud insuring agreement and the developing case law under the computer fraud insuring agreement. Section II of this paper will consider what constitutes loss of “money”, “securities” and “other property” under the computer fraud insuring agreement and how courts have interpreted these terms. Section III of this paper will discuss how courts have determined what constitutes a computer. Section IV of this paper will address how courts have analyzed what is considered a computer fraud. Section V of this paper will explore issues relating to “direct loss” under the computer fraud insuring agreement. Section VI of this paper will discuss the exchange or purchase exclusion. Section VII of this paper will address the proprietary information exclusion. Section VIII will explore the acts of employees or authorized representatives exclusion.

II. WHAT CONSTITUTES MONEY, SECURITIES OR OTHER PROPERTY?

As discussed in Section I above, most computer fraud coverage provisions will provide that the coverage applies to loss of or damage to “money”, “securities” and “other property”. “Money” may be defined as “a. Currency, coins and bank notes in current use and having a face value; and b. Travelers checks, register checks and money orders held for sale to the public.”² “Securities” may be defined as:

. . . negotiable and nonnegotiable instruments or contracts representing either “money” or property and includes:

- a. Token, tickets, revenue and other stamps (whether represented by actual stamps or unused value in a meter) in current use; and
- b. Evidences of debt issued in connection with credit or charge cards, which cards are not issued by you;

but does not include “money”.³

“Other property” may be defined as “any tangible property other than ‘money’ and ‘securities’ that has intrinsic value. . . .”⁴ While the terms “money”, “securities” and “other property” will likely be defined in the applicable policy, courts have sometimes struggled to apply these definitions to certain types of losses.

In *Royal American Group, Inc. v. ITT Hartford*,⁵ a court considered whether unauthorized access to a telephone network constituted “money”, “securities” or “other

² See ISO Form CR 00 21 07 02; ISO Form CR 00 23 05 06.

³ See ISO Form CR 00 21 07 02; ISO Form CR 00 23 05 06.

⁴ See ISO Form CR 00 21 07 02; ISO Form CR 00 23 05 06.

⁵ No. 16246, 1994 WL 14888 (Ohio App. Jan. 12, 1994).

property". The insured company provided customers with access to a long distance telephone network, through its contracts with long distance carriers, in exchange for a fee. The customers accessed the network by using a security code, which code was stored in a computer located on the insured's premises. An individual accessed the insured's computer through the use of another computer and stole the security code. The security code was used to gain unauthorized access to the telephone network, causing charges to the insured's accounts with the long distance carriers. After ITT denied the claim, the insured brought suit for breach of contract and the trial court granted summary judgment in favor of the insured. On appeal, ITT argued that the trial court erred in finding that the insured's contracts with the long distance carriers constituted "securities". The policy at issue included, as covered property, "Money", "Securities" and "property other than Money and Securities". There was no dispute between the parties that the loss was not of Money or property other than Money and Securities. The trial court had held that the contracts, which represented the right to utilize the property of the long distance carrier, were "other property" as defined under "securities". The appellate court reversed, holding that the plain meaning of the policy language definition of "securities" did not apply to the contracts. In making this determination, the court examined the language of the policy as well as dictionary definitions of securities. It reasoned that the contractual right to access another company's long distance network was not encompassed in "securities".

In *Brightpoint, Inc. v. Zurich American Insurance Co.*,⁶ one of the issues the court considered was whether phone cards constituted covered property under a crime policy. Brightpoint's business included wholesale distribution of prepaid mobile telephone cards. Brightpoint made a claim under its policy with Zurich based upon the alleged theft of phone cards, and Zurich denied the claim. On summary judgment, one of Zurich's arguments was that the phone cards were not "Money", "Securities" or "Property Other than Money and Securities". The court reasoned that the only requirement for property to fall under the definition of "Property Other than Money and Securities" was that it be tangible, have intrinsic value and not be specifically listed as not covered. Zurich argued that the loss was purely the economic value of the phone cards, not the cards themselves, and that the cards were therefore not tangible property. The court held that the phone cards each had a specific value assigned to it and were tangible and could be physically transferred to another. Therefore, it held that the phone cards fell under the policy definition of "Property Other than Money and Securities".

In *People's Telephone Co., Inc. v. Hartford Fire Ins. Co.*,⁷ the court considered whether combinations of electronic serial numbers and mobile phone identification numbers used to activate and use cellular phones were covered property under a crime insurance policy. An employee of the insured stole lists containing such combinations and sold them to third parties, who used the combinations to program other cellular phones, allegedly causing the insured to incur charges for unauthorized telephone usage. On summary judgment, the court considered whether the combinations constituted "property other than money and securities" under a policy which defined such other property as "any tangible property other than money and securities that has intrinsic value". The court also examined the Black's Law Dictionary definitions of "tangible property" and "intrinsic". The court held that the only tangible property

⁶ No. 1:04-CV-2085-SEB-JPG, 2006 WL 693377 (S.D. Ind. 2006).

⁷ 36 F.Supp.2d 1335 (S.D. Fla. 1995).

at issue was the lists of combinations and that the damages sought related to the economic value of the tangible property, which it found to be intangible. Therefore, the court held that the lists were not tangible property within the meaning of the policy.

Although most policies define “money”, “securities” and “other property”, these definitions are subject to different interpretations by courts. In determining whether a particular loss falls within these definitions, most courts examine the language of the policy itself as well as dictionary definitions and general understanding of the terms.

III. WHAT IS A COMPUTER?

Although central to the computer fraud coverage provision is the use of a computer, most crime policies do not contain a definition of “computer”. While it may seem evident what would be considered a computer, under certain circumstances, it is not entirely clear.

In *Brightpoint Inc. v. Zurich American Insurance Co.*,⁸ the court did not specifically consider, though it commented on, what might constitute a computer. The insured argued that use of facsimile machine constituted use of a computer under the applicable crime policy. The insured provided the court with an expert report in support of this theory. While not directly deciding the issue, the court noted that the “common and ordinary meaning of computer as widely used and understood in our society and around the world is severely stretched by the inclusion of a facsimile machine.”⁹

In contexts other than crime coverage, such as in the interpretation of computer crime statutes, courts have considered what constitutes a computer or what constitutes access to a computer. For instance, in *State v. Rowell*,¹⁰ a court considered whether the use of a telephone network that employs computerized switches constituted access to a computer under a state computer fraud statute. The defendant in *Rowell* telephoned various individuals, identified himself as an attorney, and advised the individuals that they were entitled to an award from a class action lawsuit and instructed each of them to wire money to him for court costs. The long distance telephone calls were processed by various computerized switches. The prosecution argued that the switches were controlled by computers and therefore fell within the definition of a computer or computer network. The defendant argued that the use of a telephone to communicate with another person was not a computer fraud. Both the district court and court of appeals held that the use of a telephone to access a long distance communications network was accessing a computer for purposes of the state computer crime statute. The Supreme Court of New Mexico disagreed. It reasoned that the defendant did not attempt to introduce fraudulent data into a computer and did not attempt to steal information from a computer, but rather used a telephone, which used computerized switches to perform the work of a telephone network. It held that such use of the computerized switches to make a telephone call did not fall under the computer crime statute.

⁸ No. 1:04-CV-2085-SEB-JPG, 2006 WL 693377 (S.D. Ind. 2006).

⁹ *Id.* at *7 n.5.

¹⁰ 908 P.2d 1379 (N.M. 1995).

However, in *People v. Rice*,¹¹ a court determined that a telephone line that was connected to an interactive computer system was a computer system and that calling the line and entering responses by telephone constituted “accessing” a computer system. The criminal defendant in *Rice* was found to have filed for unemployment compensation benefits by utilizing the Department of Labor’s interactive computer system, which allowed the claimants to communicate over the telephone. When the defendant contacted the system via telephone, it asked her if she had worked during the week for which was claiming benefits and she pressed the digit corresponding with no. In actuality, the defendant was working during that time period. The defendant was charged with a computer crime on the basis that she accessed a computer for the purpose of obtaining money from the Department of Labor or committing theft. After a jury trial, the defendant was convicted of a computer crime. She appealed, arguing that the evidence did not establish that she “accessed” a computer system and that making a telephone call and pressing telephone buttons in response to questions was not accessing a computer. On appeal, the court relied upon testimony by an employee of the Department of Labor that the line was a computerized system that used interactive voice response technology. The court determined that the trial testimony regarding the nature of the line was sufficient to support a finding that it was a “computer system” and that the defendant had accessed the computer system by communicating directly with the line by inputting data in response to computer-generated questions. Likewise, in *Commonwealth v. Gerulis*,¹² a court held that accessing a voice mailbox constitutes accessing a computer. The defendant in *Gerulis* was accused of infiltrating the voice mailbox systems of two entities, which infiltration ousted the authorized users from their voice mailboxes. The defendant was found guilty of unlawful use of a computer. On appeal, the defendant argued there was not sufficient evidence to convict her of unlawful use of a computer. The court held that that a voice mailbox was a computer as defined under state statute because the telephone was linked to a sophisticated computerized communication system, including a computerized electronic message answering system and hard disk drive.

While it may at first blush appear obvious what a “computer” is and what it means to “use” a computer, as is demonstrated by several courts’ interpretations of what constitutes a computer and access to a computer under state computer crime laws, the answer is not always so obvious.

IV. WHAT IS COMPUTER FRAUD?

As set forth in Section I above, most computer fraud coverage provisions will contain language similar to a requirement that the loss result directly from “the use of any computer to fraudulently cause a transfer of that property from inside the ‘premises’ . . . [t]o a person. . . outside those ‘premises’; or [t]o a place outside those ‘premises’.”¹³

¹¹ 198 P.3d 1241 (Colo. Ct. App. 2008).

¹² 616 A.2d 686 (1992), *appeal denied*, 633 A.2d 150 (1993).

¹³ See ISO Form CR 00 21 07 02; ISO Form CR 00 23 05 06.

In *Milwaukee Area Technical College v. Frontier Adjusters of Milwaukee*,¹⁴ the Court of Appeals of Wisconsin considered whether a claim fell within the Computer Fraud Coverage. In that case, a college hired a third party agent to evaluate the college's workers' compensation claims and to pay the approved claims. The agent perpetrated a scam whereby he told the college he had sent checks to health care providers, when he had not done so, and then kept the reimbursement checks sent to him by the college. The agent sent dummy check ledgers to the college that represented he had paid the health care providers. The insured college sought coverage under various provisions of its policy with St. Paul Travelers, including the Computer Fraud coverage provision. The insured based this claim on the fact that the perpetrator of the fraud used a computer to print the ledgers which he sent to the college seeking reimbursement and used a computer to manage the bank account into which he put the college's funds and from which he issued checks as part of his scheme. The court did not determine whether such actions brought the claim within the Computer Fraud coverage because it determined that the exclusion for dishonest or criminal acts of the insured's authorized representatives applied to exclude coverage.

The argument advanced by the insured in *Milwaukee Area Technical College* would mean that any time a document created on a computer was a part of causing a loss, the computer fraud insuring agreement would apply. This is clearly well beyond the coverage intended by the computer fraud insuring agreement. Given the prevailing use of computers on a day to day basis by individuals and businesses, such an interpretation would bring within the scope of the coverage incidents not at all related to computer hacking or using a computer to cause a loss. While such an argument seems to defy common sense, insureds may advance such arguments when faced with a lack of coverage and the connection of a computer to the loss in some manner.

V. DIRECT LOSS

Another issue that may arise in determining whether a claim falls within the computer fraud coverage is whether the alleged loss was directly caused by use of a computer or computer fraud. While the computer fraud coverage is intended to cover incidents where a computer is hacked, resulting in the loss of money or property to an insured, an insured may attempt to make an argument that more attenuated use of a computer is sufficient to invoke the computer fraud coverage.

For instance, in *Brightpoint, Inc. v. Zurich American Insurance Co.*,¹⁵ the insured sought coverage under the computer fraud provision of a crime policy under circumstances that did not involve the unauthorized use or hacking of a computer. The insured, Brightpoint, regularly sold large volumes of phone cards to a dealer, Genato. It typically accepted payment from Genato by post-dated checks with bank guaranties certifying the sufficiency of funds in Genato's account. Genato would fax copies of the checks, bank guaranties and purchase orders to Brightpoint and Brightpoint would then purchase the phone cards and deliver them to Genato in exchange for the original checks, guaranties and purchase order. On two consecutive days, Brightpoint received copies of purchase orders, post-dated checks and bank

¹⁴ 752 N.W.2d 396 (Wis. 2008).

¹⁵ No. 1:04-CV-2085-SEB-JPG, 2006 WL 693377 (S.D. Ind. 2006).

guaranties believed to be from Genato by facsimile. Brightpoint sent one of its employees to purchase the phone cards at a distributor's office. Immediately after purchasing the cards, Brightpoint's employee met with a person he believed to be a representative of Genato and turned the cards over to him after receiving originals of the post-dated checks and guaranties previously faxed. Genato later denied issuing the purchase orders and denied authorizing the representative to pick up the phone cards. Brightpoint was never paid for the phone cards and made a claim under its policy with Zurich. Zurich denied the claim on the basis that there was no evidence submitted that a computer was used to fraudulently cause the transfer of phone cards and therefore there was no covered loss.

On summary judgment, one of Zurich's arguments was that the faxed post-dated checks and bank guaranties did not fraudulently cause a transfer of the phone cards. The court agreed with Zurich that the receipt of the facsimile transmission was not the cause of Brightpoint's loss. The court reasoned that it was only after receipt of the original documents that Brightpoint would release the cards and they would not have been released only on the basis of the facsimile. The court further noted that the fraud occurred through the use of unauthorized checks and guaranties, not the manipulation of numbers or events through the use of a computer. It held that, while the facsimile transmission caused Brightpoint to purchase the cards from its supplier, it did not cause it to transfer the cards and therefore did not directly or proximately cause the theft. Brightpoint argued that the policy only required that the theft follow and be directly related to the use of a computer and that the policy did not require that the use of a computer be the proximate cause or predominate cause of the loss. It further argued that all that was required for coverage was the use of a computer followed by a theft in some way connected to the use of the computer. The court rejected that argument and noted that Brightpoint's interpretation of the term "directly related" represented a distortion of the policy terms. The court looked to the Black's Law Dictionary definition of "directly" as "in a straight line or course" and "immediately". The court further reasoned that, applying Brightpoint's interpretation, coverage would be provided where a customer sends an e-mail saying he is coming to the office to make a purchase of phone cards and then comes to the office and completes the transaction with the use of counterfeit money. The court noted that, if coverage were allowed under this hypothetical, it would reflect an interpretation other than a plain and ordinary interpretation of the policy and any reasonable person would not give the coverage for computer fraud that spin. The court held that both in its example and under the facts of the case, intervening events became the direct and proximate cause of the loss.

In *Great American Insurance Co. v. AFS/IBEX Financial Services, Inc.*,¹⁶ a court considered whether a loss fell within a computer fraud provision, along with various other provisions of a crime policy. The alleged loss involved an unauthorized representative of an insurance agent submitting false applications for premium financing to the insured and then depositing the checks issued to the agency by the insured into his own personal bank account. The court's decision does not contain much analysis of the Computer Fraud provision, though it did grant the insurer summary judgment with respect to coverage under the Computer Fraud provision, finding the insured failed to present an issue of fact that a computer caused the transfer of any funds from the insured's bank account.

¹⁶ No. 3:07-CV-924-O, 2008 WL 2795205 (N.D. Tex. July 21, 2008).

VI. EXCHANGE OR PURCHASE EXCLUSION

Many computer fraud insuring agreements contain an exclusion for exchanges or purchases. Such an exclusion may provide that the insuring agreement does not apply to “[l]oss resulting from the giving or surrendering of property in any exchange or purchase.”¹⁷ Other policies may similarly provide that the policy does not cover “loss resulting directly or indirectly from the giving or surrendering of Money, Securities or Other Property in any exchange or purchase, whether or not fraudulent, with any other person not in collusion with an Employee. . . .” or “loss due to an Insured knowingly having given or surrendered Money, Securities or Property in any exchange or purchase with a Third Party, not in collusion with an Employee. . . .”

In *Harrah’s Entertainment, Inc. v. ACE American Insurance*,¹⁸ a court considered whether an exchange or purchase exclusion applied to preclude coverage. In *Harrah’s*, a patron presented the casino with fraudulent cashier’s checks, which were accepted by the casino in exchange for that amount in gambling credit. After the patron lost over \$1.4 million of the gambling credit and cashed out the \$38,200, Harrah’s discovered that the cashier’s checks were fraudulent. The policy contained an exclusion providing that coverage did not apply to the “giving or surrendering of Money or Securities in any exchange or purchase.”¹⁹ The court found that Harrah’s had given or surrendered gambling credit, which constituted “Money or Securities”, in exchange for the forged checks. It therefore determined that the exchange or purchase exclusion applied to exclude coverage.

VII. PROPRIETARY INFORMATION EXCLUSION

Some computer fraud insuring agreements provide an exclusion for proprietary or confidential information. Such an exclusion might state the policy does not cover:

Loss resulting from:

- (1) The unauthorized disclosure of your confidential information including, but not limited to, patents, trade secrets, processing methods or customer lists;
or
- (2) The unauthorized use or disclosure of confidential information of another person or entity which is held by you including, but not limited to, financial information, personal information, credit card information or similar non-public information.²⁰

A variation may provide that the policy does not cover “[l]oss resulting directly or indirectly from any Theft, disappearance, damage, destruction or disclosure of any tangible property or

¹⁷ See ISO Form CR 00 21 07 02.

¹⁸ 100 Fed. Appx. 387 (6th Cir. 2004).

¹⁹ *Id.* at 390.

²⁰ See ISO Form CR 00 23 05 06.

confidential information including . . . trade secret information, confidential processing methods or other confidential information or intellectual property. . . “ or “loss of trade secrets, confidential processing methods or other confidential information of any kind. . . .”

In *Retail Ventures, Inc. v. National Union Fire Insurance Co. of Pittsburgh, Pennsylvania*,²¹ an insured brought suit after coverage for a computer hacking incident was denied based upon a proprietary information exclusion. The insured, whose subsidiaries, DSW, Inc. and DSW Shoe Warehouse, were in the retail shoe business, made a claim under its consumer fraud insurance policy after there had been unauthorized access and theft of customer data on retail store and corporate computer systems. National Union denied the claim, in part based upon a proprietary information exclusion which excluded coverage for “proprietary information, Trade Secrets, Confidential Processing Methods or other confidential information of any kind.”²² The court did not reach the issue of whether the proprietary information exclusion applied in this context.

VII. ACTS OF EMPLOYEES OR AUTHORIZED REPRESENTATIVES EXCLUSION

Some computer fraud insuring agreements provide an exclusion for acts of employees or authorized representatives. Such an exclusion might state the policy does not cover:

Loss resulting from “theft” or any other dishonest act committed by any of your “employees”, “managers”, directors, trustees or authorized representatives:

(1) Whether acting alone or in collusion with other persons; or

(2) While performing services for you or otherwise;²³

In *Milwaukee Area Technical College v. Frontier Adjusters of Milwaukee*,²⁴ the court considered whether an authorized representatives exclusion operated to exclude coverage for a claim made under the computer fraud insuring agreement. In that case, also discussed in Section IV above, a college hired a third party agent to evaluate the college’s workers’ compensation claims and to pay the approved claims. The agent perpetrated a scam whereby he told the college he had sent checks to health care providers, when he had not done so, and then kept the reimbursement checks sent to him by the college. The agent sent dummy check ledgers to the college that represented he had paid the health care providers. The insured college sought coverage under various provisions of its policy with St. Paul Travelers, including the Computer Fraud coverage provision. The St. Paul Travelers policy contained an exclusion providing that the computer fraud insuring agreement did not apply to “[l]oss resulting from any dishonest or criminal acts committed by any of your ‘Employees’, directors, trustees or authorized representatives whether acting alone or in collusion with other persons or while

²¹ No. 2:06-CV-00443, 2007 WL 943011 (S.D. Ohio Mar. 27, 2007).

²² *Id.* at *1.

²³ See ISO Form CR 00 23 05 06.

²⁴ 752 N.W.2d 396 (Wis. 2008).

performing services for you or otherwise.”²⁵ The court stated there was no dispute that the third party agent was the college’s authorized representative in connection with the workers’ compensation matter. The insured argued that, because it had not authorized the third party agent to steal from it, the agent was not the college’s authorized representative. The court held that the insured’s argument was circular and would also wholly abrogate the exclusion as the exclusion would never apply under the insured’s reasoning, because every time a representative stole from the insured, the theft would not be authorized.²⁶

VIII. CONCLUSION

Though the computer fraud insuring agreement has existed in commercial crime policies for some time, the reported case law interpreting the computer fraud insuring agreement is sparse. However, cases under the computer fraud insuring agreement indicate that insureds are attempting to invoke coverage under the computer fraud insuring agreement for incidents beyond what would traditionally be thought of as hacking or computer fraud. In analyzing such claims, the language of the computer fraud insuring agreement itself, including the requirement of “direct loss”, will be significant, as will the various exclusions that may apply to the computer fraud coverage.

²⁵ *Id.* at 402.

²⁶ *Id.*

SUSAN EVANS JONES is an associate with the firm Wolf, Horowitz & Etlinger, LLC in Hartford, Connecticut. Her practice focuses on surety and fidelity, and insurance coverage and defense. Susan received her undergraduate degree from Skidmore College (B.A., cum laude, 1999). She received her law degree from the University of Connecticut School of Law (J.D., with high honors, 2004).

She can be reached by phone at 860-724-6667 or by email at sevans@wolfhorowitz.com.